REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. <u>Rejection of Claim 1 Under 35 USC §112, 2nd Paragraph</u>

This rejection has been addressed by amending claim 1 to clarify that the client is in fact configuring the "other network apparatus" using NEAP, as suggested in the last sentence of item 2 of the Official Action.

2. <u>Rejection of Claim 6 Under 35 USC §112, 1st Paragraph</u>

This rejection is respectfully traversed on the grounds that the subject matter of claim 6 is set forth in detail in lines 10 *et seq.* on page 6 of the original specification. A copy of page 6 is attached hereto in case page 6 is missing from the Examiner's file.

3. <u>Rejection of Claims 1-6 Under 35 USC §103(a) in view of "*An Algorithm For Topology Discovery Of IP Networks*" (Lin) and U.S. Patent No. 6,618,755 (Bonn)</u>

This rejection is respectfully traversed on the grounds that neither the Lin article nor the Bonn patent discloses or suggests a network apparatus management protocol (NEAP) in which, as recited in claim 1:

- a network management tool is arranged to configure network devices *by serving as a client*, the network devices playing the role of multiple servers to the network management tool's single client, and

- the multiple "servers," *i.e.*, the network devices or apparatuses, each send UDP packets to the "client," the UDP packets containing a source port number that identifies the client and a "special communication port number" that enables the network devices to carry out and respond to management request simply by broadcasting to a common IP and MAC destination address.

Furthermore, neither the Lin publication nor the Bonn patent even remotely suggests that setting and getting should be accomplished through the use of attribute columns in the UDP packet, as recited in claims 4 and 5, or the inclusion of an authenticator column as recited in claim 6.

Instead of causing network devices to act as "servers" to a network management tool's "client," the Lin publication teaches use of SNMP (which is described on pages 1-2 of the present application as "prior art") to find subnet IDs (and connections therebetween) from MIB information stored in network routers. The routers of Lin do not correspond to the claimed "network apparatuses" since routers do not assign port numbers to a UDP header, much less in a request packet to a "client" as claimed, and the "topology" data collected from the MIBs in the routers clearly do not correspond to source or destination **port numbers**, but rather are in the form of **IP addresses**.

These deficiencies are not remedied by the Bonn patent, which also concerns identification of subnet nodes based on **IP addresses** stored in routers. Neither the Bonn patent nor the Lin publication describes a system that affects the port numbers included in UDP packets sent by network apparatuses. In fact, neither the Bonn system nor the Lin system operates at, or is able to operate at, the UDP or transport level.

The claimed invention does not seek to identify **subnet** nodes whose addresses are not previously known, as in the Lin publication or the Bonn patent, but rather seeks to identify MAC addresses and device attributes in order to facilitate network setting (and getting) operations by modifying SNMP such as that the network management software functions as a client rather than a server, thereby enabling getting or setting operations with respect to individual devices to be conducted through "broadcasts" from the network devices to the management tool. **Enabling the network devices to broadcast the information simplifies the collecting the "search" or collection of information, without any need to resort to MIBs, test packets, or the like.**

7

In this regard, it is significant that the NEAP of the invention operates at the **transport layer**, *i.e.*, at the hardware (port) level, inside the ISO/OSI mode (as explained in line 5 on page 5 of the original specification), and works by assigning a **special communication port number** in the UDP header as the port number for every server, which can then be used to receive a request from the network management software at the "client end." This allows the requests to be transmitted by broadcasting, in which case all of the IP destination addresses of the servers are set as 255.255.255.255 and the MAC destination addresses thereof are set as FF; FF; FF; FF; FF; FF, *which means that there is no possible need for reference to MIBs as in the Lin publication, or the sending of test packets as in the Bonn patent.* Neither the Lin nor Bonn suggests any sort of modification of the conventional SNMP, much less one that manipulates port information in a UDP header, as claimed, to enable management by broadcasting *from the network devices* (which serve as servers).

According to the claimed invention,. An assigned special UDP communication port number is used as the UDP destination port number, the UDP source port number is set according to a mechanism of the client, and every "server" is caused conduct a requested management operation according to the contents of the packet after every server receives the request packet, exchanges the UDP destination port number and source port number, and transmits the packet back to the client by broadcasting. As a result, the management tool (client) can continuously distribute three packets requesting a search through the set proper time interval, such as every 3 seconds, permitting the client to rapidly upgrade firmware of the network devices as soon as the request packets have been received by and filled in by the network devices with related data, such as the model number and MAC address thereof, and transmitted back to the client. Nowhere do the Lin publication and Bonn patent even remotely suggest such data collection for network management purposes.

Finally, with respect to claim 6, neither Lin nor Bonn suggests the claimed code encryption method which adds a password to the entire request packet sent from the client, excluding columns of an authenticator and server MAC address, and encrypts it into data that
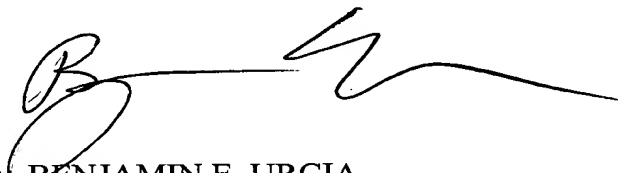
fills the authenticator column before sending the request packet out from the client. This method is necessary because of the manner in which each network device acts as a server in broadcasting data for setting and getting operations. In contrast, the Lin patent does not mention any data security, while the cited passages in the Bonn patent merely mention that protected computer systems need to be protected from unauthorized packets. There is <u>no</u> suggestion in either patent of the claimed authenticator column of the UDP packet, use of the MAC address in the claimed manner, or any other feature of the encryption/authentication scheme recited in claim 6.

For the foregoing reasons, it is believed that the rejection of claims 1-6 under 35 USC §103(a) is improper and withdrawal of the rejection is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: February 23, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beu\Pending Q...Z\Y\YU 894128\a01.wpd

9

the UDP source port number, then transmits the said packet back to the said client end by broadcasting. Therefore, the client end can continuously distribute three packets requesting for conducting search through the set proper time interval (such as every 3 seconds); after the said request packet being received by the said every server, the said

5   every server fills the related data, such as the model number and MAC address of the server product, of the said every server in the said packet right away and transmits the said packet back to the client end, referring to FIG. 5 for the procedures, to enable the client end installed with the NEAP to rapidly search all the network apparatuses capable of executing the said NEAP on the network.

10   In the present invention, when trying to conduct getting or setting for the said every server via the said NEAP, the said every server has to possess the ability of recognizing and identifying the password; before being sent out by the said client end, the said password has to be encrypted in codes for preventing the network hacker from stealing the password; the common method of code encryption is a code encryption

15   method called MD5; the said MD5 code encryption method adds the password to the entire request packet sent from the client end excluding the columns of authenticator and server MAC address and encrypts it into 16-bit data, fills the said 16-bit data in the said authenticator column, then sends the said request packet out from the client end. After the said request packet being received by the said every server (those with the

20   same MAC address as that of the server MAC address column in the said request packet), the said every server uses the same MD5 code encryption method to encrypt the entire request packet into 16-bit data according to the preset password provided by the said every server, then compares it with the data in the authenticator column in the request packet sent from the client end; if both are the same, the operation of getting or

25   setting is conducted; otherwise, the request of the said packet is rejected; therefore, the